

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 7,657,748 B2
APPLICATION NO. : 10/521741
DATED : February 2, 2010
INVENTOR(S) : Craig B. Gentry

Page 1 of 2

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the Title Page:

The first or sole Notice should read --

Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1404 days.

Column 8, Line 34: delete "(PKB, SKB)"; insert --(PK_B, SK_B)--.

Column 8, Line 44: delete the word "params"; insert --*params*--.

Column 8, Line 45: delete the words "masks S"; insert --masks *s*--.

Column 8, Line 46: delete the word "ID"; insert --*ID*--.

Column 8, Line 50 & 51: delete the words "s, params and ID"; insert --*s, params* and *ID*--.

Column 8, Line 52: delete the word "ID"; insert --*ID*--.

Column 8, Line 54: delete the words "params, ID and M"; insert --*params, ID* and *M*--.

Column 8, Line 55: delete the words "C to recover M"; insert --*C* to recover *M*--.

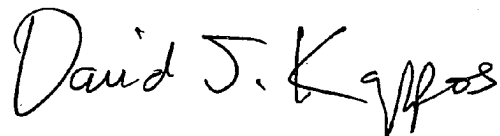
Column 10, Line 61 & 62: delete " $\hat{e}(P, P)^{abc}$ if P , aP , bP , and cP are known, but a , b , and c are not";
insert -- $\hat{e}(P, P)^{abc}$ if P , aP , bP , and cP are known, but a , b , and c are not--.

Column 10, Line 64 & 65: delete " $\hat{e}(P, P)^{abc} = \hat{e}(abP, cP)$ "; insert -- $\hat{e}(P, P)^{abc} = \hat{e}(abP, cP)$ --.

Column 10, Line 66 & 67: delete " $g = \hat{e}(P, P)$, then $g^{abc} = g^{ab)c}$ where $g^{ab} = \hat{e}(aP, bP)$ and $g^c = \hat{e}(P, cP)$ ";
insert -- $g = \hat{e}(P, P)$, then $g^{abc} = (g^{ab})^c$ where $g^{ab} = \hat{e}(aP, bP)$ and $g^c = \hat{e}(P, cP)$ --.

Signed and Sealed this

Twenty-first Day of December, 2010



David J. Kappos
Director of the United States Patent and Trademark Office

Column 11, Line 48: delete “ $C = [rP, M \oplus H_2(g^l)]$, where $g = \hat{e}(Q, P_B) \in G_2$ ”;
insert -- $C = [rP, M \oplus H_2(g^l)]$, where $g = \hat{e}(Q, P_B) \hat{e}(s_B P, P'_B) \in G_2$ --.

Column 12, Line 59: delete the word “params”; insert --*params*--.

Column 13, Line 39: delete the word “params”; insert --*params*--.

Column 13, Line 43: delete the word “Musing”; insert --*M* using--.

Column 15, Line 7: delete the word “sendery”; insert --sender *y*--.

Column 15, Line 11: delete the word “sendery”; insert --sender *y*--.

Column 15, Line 60: delete “ $m-1+1$ ”; insert -- $m-l+1$ --.

Column 15, Line 66: delete “ $1-1$ ”; insert -- $l-1$ --.

Column 16, Line 10: delete “ $n-1+1$ ”; insert -- $n-l+1$ --.

Column 16, Line 17: delete “ $1-1$ ”; insert -- $l-1$ --.

Column 16, Line 25: delete “ $n-1$ ”; insert -- $n-l$ --.

Column 19, Line 37: delete “sendery”; insert --sender *y*--.

Column 20, Line 19: delete “ $U_1 = rP_{zi}$ for $k+1 \leq i \leq n+1$ ”; insert -- $U_i = rP_{zi}$ for $l+1 \leq i \leq n+1$ --.

Column 24, Line 40: delete the word “params”; insert --*params*--.

Claim 80 line 8 (Column 38, Line 11): delete “key!recipient”; insert --key/recipient--.

Claim 80 line 21 (Column 38, Line 24): delete “key!private”; insert --key/private--.